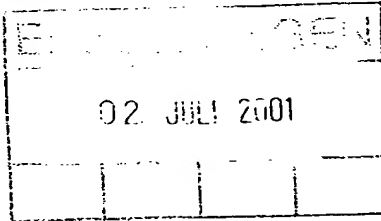


VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESEN

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN
PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

SCHOPPE, Fritz
SCHOPPE, ZIMMERMANN & STÖCKELER
Postfach 71 08 67
D-81458 München
ALLEMAGNE



IPER
PCT

MITTEILUNG ÜBER DIE ÜBERSENDUNG
DES INTERNATIONALEN VORLÄUFIGEN
PRÜFUNGSBERICHTS
(Regel 71.1 PCT)

Absendedatum
(Tag/Monat/Jahr) 29.06.2001

Aktenzeichen des Anmelders oder Anwalts
FH991205PCT

WICHTIGE MITTEILUNG

Internationales Aktenzeichen
PCT/EP99/09978

Internationales Anmeldedatum (Tag/Monat/Jahr)
15/12/1999

Prioritätsdatum (Tag/Monat/Jahr)
24/02/1999

Anmelder

FRAUNHOFER-GESELLSCHAFT ...et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.
2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.
3. Auf Wunsch eines ausgewählten Amtes wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

4. ERINNERUNG

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung
beauftragten Behörde



Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Le Nadan, M

Tel. +49 89 2399-2350



VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts FH991205PCT	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP99/09978	Internationales Anmeldedatum (Tag/Monat/Jahr) 15/12/1999	Prioritätsdatum (Tag/Monat/Jahr) 24/02/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04K1/00		
Anmelder FRAUNHOFER-GESELLSCHAFT ...et al.		



1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
2. Dieser BERICHT umfaßt insgesamt 10 Blätter einschließlich dieses Deckblatts.

☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 24 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☒ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 22/09/2000	Datum der Fertigstellung dieses Berichts 29.06.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Willems, B Tel. Nr. +49 89 2399 8954 

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1,2,4-24 ursprüngliche Fassung

3,3a-3b eingegangen am 07/06/2001 mit Schreiben vom 07/06/2001

Patentansprüche, Nr.:

1-36 eingegangen am 07/06/2001 mit Schreiben vom 07/06/2001

Zeichnungen, Blätter:

1/8-8/8 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/09978

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

IV. Mangelnde Einheitlichkeit der Erfindung

1. Auf die Aufforderung zur Einschränkung der Ansprüche oder zur Zahlung zusätzlicher Gebühren hat der Anmelder:

- ☐ die Ansprüche eingeschränkt.
- ☐ zusätzliche Gebühren entrichtet.
- ☐ zusätzliche Gebühren unter Widerspruch entrichtet.
- ☐ weder die Ansprüche eingeschränkt noch zusätzliche Gebühren entrichtet.

2. ☒ Die Behörde hat festgestellt, daß das Erfordernis der Einheitlichkeit der Erfindung nicht erfüllt ist, und hat gemäß Regel 68.1 beschlossen, den Anmelder nicht zur Einschränkung der Ansprüche oder zur Zahlung zusätzlicher Gebühren aufzufordern.

3. Die Behörde ist der Auffassung, daß das Erfordernis der Einheitlichkeit der Erfindung nach den Regeln 13.1, 13.2 und 13.3

- ☐ erfüllt ist
- ☒ aus folgenden Gründen nicht erfüllt ist:
siehe Beiblatt

4. Daher wurde zur Erstellung dieses Berichts eine internationale vorläufige Prüfung für folgende Teile der internationalen Anmeldung durchgeführt:

- ☒ alle Teile.
- ☐ die Teile, die sich auf die Ansprüche Nr. beziehen.

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/09978

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1 - 36
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1 - 24
	Nein: Ansprüche	25 - 36
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1 - 36
	Nein: Ansprüche	

2. Unterlagen und Erklärungen siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

Zu Punkt IV

Mangelnde Einheitlichkeit der Erfindung

1. Zitiertes Dokument:

D1 = QUACKENBUSH ET AL.: 'Noiseless Coding of Quantized Spectral Components in MPEG-2 Advanced Audio Coding' 1997 IEEE ASSP WORKSHOP ON APPLICATIONS OF SIGNAL PROCESSING TO AUDIO AND ACOUSTICS, 19. Oktober 1997 (1997-10-19)

2. Die verschiedenen Gruppen von Erfindungen sind: Ansprüche 1 bis 24 und Ansprüche 25 bis 36.

Aus den folgenden Gründen hängen diese Gruppen nicht so zusammen, daß sie eine einzige allgemeine erfinderische Idee verwirklichen (Regel 13.1 PCT):

Dokument D1 beschreibt (siehe Figur 1) eine Vorrichtung zum Codieren eines Datenstroms aus einem Audiosignal, mit den Merkmalen des in den Ansprüchen aufgeführten Codierers.

Die erstgenannte Gruppe beansprucht weiter eine Verschlüsselung des Signals durch Umsortieren der quantisierten Spektralwerten, die zweitgenannte Gruppe beansprucht weiter eine Verschlüsselung durch Umsortieren von Codewörtern.

Der technische Zusammenhang zwischen der ersten und der zweiten Gruppe besteht aus den Merkmalen des Codierers. Diese Merkmale sind aus dem Dokument D1 bekannt.

Zwischen den Merkmalen der Verschlüsselung in der ersten und in der zweiten Gruppe besteht kein technischer Zusammenhang im Sinne der Regel 13.2 PCT.

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Zitierte Dokumente:

D1 = QUACKENBUSH ET AL.: 'Noiseless Coding of Quantized Spectral Components in MPEG-2 Advanced Audio Coding' 1997 IEEE ASSP WORKSHOP ON APPLICATIONS OF SIGNAL PROCESSING TO AUDIO AND ACOUSTICS, 19. Oktober 1997 (1997-10-19)

D2 = US-A-5 796 838

D3 = US-A-4 534 037

D4 = EP-A-0 649 261

D5 = WO98/21852

D6 = US-A-5 636 279

2. Der Gegenstand des Anspruchs 1 ist in Bezug auf den im Internationalen Recherchenbericht genannten Stand der Technik neu und erfinderisch. Daher erfüllt Anspruch 1 die Erfordernisse der Artikel 33(2) und 33(3) PCT.

Dokument D1 beschreibt (siehe Figur 1) eine Vorrichtung zum Codieren eines Datenstroms aus einem Audiosignal, mit den Merkmalen des in den Ansprüchen aufgeführten Codierers.

Dokument D2 beschreibt eine Inversion eines Spektrums, derart, daß das Ausgangsspektrum gegenüber dem Eingangsspektrum invertiert ist. Die Form des Spektrums wird durch die Frequenzinversion lediglich gespiegelt, jedoch nicht

vollkommen verändert, wie es bei einer Verwüfelung der Fall sein würde.

Keines der im Recherchenbericht zitierten Dokumente gibt einen Hinweis auf die Umsortierung von quantisierten Spektralwerten in einem Frequenzband, dem eine Codetabelle einer Mehrzahl von Codetabellen zugeordnet ist.

Mit der genannten Umsortierung wird eine "weiche" Verschlüsselung erreicht, die die Datenstromsyntax des Codierers nicht verändert.

Somit ist der Gegenstand des Anspruchs 1 in Bezug auf den im Recherchenbericht genannten Stand der Technik neu und erfinderisch.

3. Der Gegenstand der Ansprüche 2 bis 10 ist in Bezug auf den im Internationalen Recherchenbericht genannten Stand der Technik neu und erfinderisch. Daher erfüllen Ansprüche 2 bis 10 die Erfordernisse der Artikel 33(2) und 33(3) PCT.

Ansprüche 2 bis 10 sind entweder direkt oder indirekt von Anspruch 1 abhängig.

4. Der Gegenstand der Ansprüche 11 bis 13 ist in Bezug auf den im Internationalen Recherchenbericht genannten Stand der Technik neu und erfinderisch. Daher erfüllen Ansprüche 11 bis 13 die Erfordernisse der Artikel 33(2) und 33(3) PCT.

Der Gegenstand der Ansprüche 11 bis 13 unterscheidet sich vom Gegenstand des Anspruchs 1 dadurch, daß erstere weitere Mittel aufweisen um die Verschlüsselung auf Basis eines ersten Schlüssels rückgängig zu machen und eine Verschlüsselung auf Basis eines zweiten Schlüssels durchzuführen.

Somit ist der Gegenstand der Ansprüche 11 bis 13 wegen den in Punkt 2 genannten Gründen neu und erfinderisch.

5. Der Gegenstand der Ansprüche 14, 15 und 16 ist in Bezug auf den im Internationalen Recherchenbericht genannten Stand der Technik neu und

erfinderisch. Daher erfüllen Ansprüche 14, 15 und 16 die Erfordernisse der Artikel 33(2) und 33(3) PCT.

Ansprüche 14, 15 und 16 sind entweder direkt oder indirekt von den Ansprüchen 11 bis 13 abhängig.

6. Der Gegenstand der Ansprüche 17 bis 19 ist in Bezug auf den im Internationalen Recherchenbericht genannten Stand der Technik neu und erfinderisch. Daher erfüllen Ansprüche 17 bis 19 die Erfordernisse der Artikel 33(2) und 33(3) PCT.

Ansprüche 17 bis 19 beziehen sich auf eine Vorrichtung zum Entschlüsseln eines Datenstroms, wobei die in Anspruch 1 definierte Umsortierung rückgängig gemacht wird.

Somit ist der Gegenstand der Ansprüche 17 bis 19 wegen den in Punkt 2 genannten Gründen neu und erfinderisch.

7. Der Gegenstand der Ansprüche 20 bis 24 ist in bezug auf den im Internationalen Recherchenbericht genannten Stand der Technik neu und erfinderisch. Daher erfüllen Ansprüche 20 bis 24 die Erfordernisse der Artikel 33(2) und 33(3) PCT.

Ansprüche 20 bis 24 definieren ein Verfahren mit Verfahrensschritten die mit den Merkmalen der vorhergehend beanspruchten Vorrichtung übereinstimmen.

Somit ist der Gegenstand der Ansprüche 20 bis 24 wegen den in Punkt 2 genannten Gründen neu und erfinderisch.

8. Der Gegenstand des Anspruchs 25 ist in Bezug auf den Inhalt der Dokumente D1 und D3 nicht erfinderisch. Daher erfüllt Anspruch 25 nicht die Erfordernisse des Artikels 33(3) PCT.

Dokument D1 beschreibt (siehe Figur 1) eine Vorrichtung zum Codieren eines Datenstroms aus einem Audiosignal, mit den Merkmalen des in den Ansprüchen aufgeführten Codierers.

Dokument D3 beschreibt eine Verschlüsselung von Audiosignalen durch Umsortieren von Bitgruppen zwischen benachbarten Codewörtern. Wird die in Dokument D3 beschriebene Frequenzumwandlung (siehe Spalte 4, Zeilen 56 - 61) nicht angestrebt, wäre es dem Fachmann naheliegend eine Verschlüsselung durch umsordieren von Codewörtern zu bewirken. Somit wird die Verschlüsselung eines Audiosignals durch Umsortieren von Codewörtern von dem Dokument D3 nahegelegt.

Der Fachmann würde zwangsläufig versuchen, die aus Dokument D1 bekannte Codierung mit der durch Dokument D3 nahegelegte Verschlüsselung zu kombinieren.

9. Der Gegenstand der Ansprüche 26, 27 ist in Bezug auf den Inhalt der Dokumente D1 und D3 nicht erfinderisch. Daher erfüllen die Ansprüche 26, 27 nicht die Erfordernisse des Artikels 33(3) PCT.

Das Zusatzmerkmal des Anspruchs 26 bezieht sich auf ein dem Fachmann geläufiges Merkmal einer Verschlüsselungseinrichtung.

Das Zusatzmerkmal des Anspruchs 27 ist aus dem Dokument D3 bekannt.

10. Der Gegenstand der Ansprüche 28 und 29 ist in Bezug auf den Inhalt der Dokumente D1, D3 und D5 nicht erfinderisch. Daher erfüllen die Ansprüche 27 und 28 nicht die Erfordernisse des Artikels 33(3) PCT.

Der Gegenstand der Ansprüche 28 und 29 unterscheidet sich vom Gegenstand des Anspruchs 25 dadurch, daß erstere weitere Mittel aufweisen um die Verschlüsselung auf Basis eines ersten Schlüssels rückgängig zu machen und eine Verschlüsselung auf Basis eines zweiten Schlüssels durchzuführen.

Der Übergang von einem ersten Schlüssel auf einen zweiten Schlüssel ist aus dem Dokument D5 bekannt. Der Fachmann würde ohne erfinderisches Zutun den Umständen entsprechend dieses Merkmal in die beanspruchte Verschlüsselungsvorrichtung aufnehmen.

11. Der Gegenstand der Ansprüche 30 und 31 ist in Bezug auf den Inhalt der Dokumente D1 und D3 nicht erfinderisch. Daher erfüllen Ansprüche 30 und 31 nicht die Erfordernisse des Artikels 33(3) PCT.

Ansprüche 30 und 31 beziehen sich auf einer Vorrichtung zum Entschlüsseln eines Datenstroms. Diese Ansprüche weisen gegenüber den Ansprüchen für die Verschlüsselungseinrichtung keine zusätzlichen Merkmale auf, die deren Gegenstand auf eine erfinderische Art und Weise vom genannten Stand der Technik unterscheiden könnten.

12. Der Gegenstand des Ansprüche 32 bis 34 ist in Bezug auf den Inhalt des genannten Stand der Technik nicht erfinderisch. Daher erfüllen Ansprüche 32 bis 34 nicht die Erfordernisse des Artikels 33(3) PCT.

Ansprüche 32 bis 34 definieren ein Verfahren mit Verfahrensschritten die mit den Merkmalen der Vorrichtungsansprüche 25 bis 31 übereinstimmen. Daher gelten die gegen Ansprüche 25 bis 31 erhobenen Einwände auch für Ansprüche 32 bis 34.

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

Ansprüche 15 and 16 sind von nachfolgenden Ansprüchen abhängig.

das Stück entschlüsseln kann. Ein Abspielgerät, das nicht den korrekten Schlüssel hat, wird, sobald es auf die verschlüsselten Multimediadaten trifft, den Betrieb einstellen. Damit ist das Ziel erreicht, daß nur der Benutzer, der autorisiert ist, ein Multimediastück abspielen kann. Diese Secure Envelope Technik stellt somit ein zweistufiges Verfahren dar, bei dem ein Multimediastück zunächst codiert wird, um eine erhebliche Datenkompression zu erreichen, und bei dem dann ein kryptographischer Algorithmus eingesetzt wird, um das codierte Multimediastück gegen unerlaubte Angreifer zu verteidigen.

Für Anwendungen, die keinen solchen Maximalschutz erfordern, ist das beschriebene Konzept darin nachteilig, daß es relativ aufwendig werden kann und wesentliche Modifikationen an Abspielgeräten erforderlich macht, um den Bestimmungsdatenblock verarbeiten zu können. Die Abspielgeräte, die letztendlich Massenprodukte im Consumer-Bereich sind, und daher preisgünstig angeboten werden müssen, sollten jedoch wenn möglich überhaupt nicht verändert werden müssen, um auch geschützte Multimediastücke abspielen zu können. Damit bleibt festzustellen, daß das bekannte Verschlüsselungskonzept zwar einen maximalen Schutz und eine hohe Verschlüsselungsflexibilität durch entsprechendes Gestalten des Anfangsblocks möglich macht, daß jedoch ebenso deutliche Veränderungen an Abspielgeräten erforderlich sind, um verschlüsselte Dateien wieder entschlüsseln bzw. überhaupt einlesen zu können.

~~Die Aufgabe der vorliegenden Erfindung besteht darin, ein anderes Konzept zum Ver- bzw. Entschlüsseln von Audio- und/oder Videosignalen zu schaffen.~~

~~Diese Aufgabe wird durch eine Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms nach Patentanspruch 1, 17 oder 18 durch eine Vorrichtung zum Erzeugen eines entschlüsselten Datenstroms nach Patentanspruch 19 oder 23, durch ein Verfahren zum Erzeugen eines verschlüsselten Datenstroms nach Patentanspruch 29 und durch ein Verfahren zum Erzeugen eines~~

-o Seite 3a

Das U.S. Patent Nr. 5,796,838 offenbart ein Verfahren und eine Vorrichtung zum Durchführen einer Inversion eines Frequenzspektrums. Die Inversion des Frequenzspektrum wird erreicht, indem ein unverschlüsseltes Audiosignal analog/digital-gewandelt wird. Das Audiosignal wird dann einer positiven komplexen Frequenzübersetzung unterzogen, so daß die negativen Frequenzkomponenten des Audiosignals um 0 Hz herum positioniert werden. Dann wird das hinsichtlich seiner Frequenz umgesetzte Audiosignal tiefpaßgefiltert, so daß nur die Basisbandkomponenten verbleiben. Das gefilterte komplexe Basisbandsignal wird dann einer beliebigen komplexen Frequenzverschiebung unterzogen, um die Signalfrequenz in einem erwünschten Frequenzband zu positionieren. Das resultierende Signal hat ein gegenüber dem ursprünglichen Audiosignal invertiertes Spektrum. Das abschließende Audiosignal wird erzeugt, indem der Realteil der komplexen Abtastwerte extrahiert wird.

Das U.S.-Patent Nr. 4,534,037 offenbart ein Verfahren und eine Vorrichtung für eine gescrambelte Puls-Code-Modulation-Übertragung oder -Aufzeichnung. Um spezielle Spektralkomponenten einer Sequenz von Digitalsignalen, die in Puls-Code-Wörtern übertragen oder aufgezeichnet werden, hervorzuheben, werden "umgepackte" Wörter gebildet, die eines oder mehrere Bits eines Worts der ursprünglichen Sequenz und eine komplementäre Anzahl von Bits von dem nächsten Wort umfassen. Die Bits eines Worts, aus dem ein "umgepacktes" Wort besteht, werden vor dem Umpacken invertiert, so daß beispielsweise die vierfache Abtastfrequenz, die doppelte Abtastfrequenz oder die Abtastfrequenz selbst in dem Spektrum hervorgehoben werden kann. Ohne Inversion von Wörtern ist es möglich, das Frequenzspektrum hinsichtlich der Frequenz nach unten zu transformieren.

Seite 3b ---->

~~das Stück entschlüsseln kann. Ein Abspielgerät, das nicht~~
den korrekten Schlüssel hat, wird, sobald es auf die verschlüsselten Multimediadaten trifft, den Betrieb einstellen. Damit ist das Ziel erreicht, daß nur der Benutzer, der autorisiert ist, ein Multimediastück abspielen kann. Diese Secure Envelope Technik stellt somit ein zweistufiges Verfahren dar, bei dem ein Multimediastück zunächst codiert wird, um eine erhebliche Datenkompression zu erreichen, und bei dem dann ein kryptographischer Algorithmus eingesetzt wird, um das codierte Multimediastück gegen unerlaubte Angreifer zu verteidigen.

Für Anwendungen, die keinen solchen Maximalschutz erfordern, ist das beschriebene Konzept darin nachteilig, daß es relativ aufwendig werden kann und wesentliche Modifikationen an Abspielgeräten erforderlich macht, um den Bestimmungsdatenblock verarbeiten zu können. Die Abspielgeräte, die letztendlich Massenprodukte im Consumer-Bereich sind, und daher preisgünstig angeboten werden müssen, sollten jedoch wenn möglich überhaupt nicht verändert werden müssen, um auch geschützte Multimediastücke abspielen zu können. Damit bleibt festzustellen, daß das bekannte Verschlüsselungskonzept zwar einen maximalen Schutz und eine hohe Verschlüsselungsflexibilität durch entsprechendes Gestalten des Anfangsblocks möglich macht, daß jedoch ebenso deutliche Veränderungen an Abspielgeräten erforderlich sind, um verschlüsselte Dateien ~~wieder entschlüsseln bzw. überhaupt einlesen zu können.~~

Die Aufgabe der vorliegenden Erfindung besteht darin, ein anderes Konzept zum Ver- bzw. Entschlüsseln von Audio- und/oder Videosignalen zu schaffen.

Diese Aufgabe wird durch eine Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms nach Patentanspruch 1, 17 oder 18 durch eine Vorrichtung zum Erzeugen eines entschlüsselten Datenstroms nach Patentanspruch 19 oder 23, durch ein Verfahren zum Erzeugen eines verschlüsselten Datenstroms nach Patentanspruch 29 und durch ein Verfahren zum Erzeugen eines

Patentansprüche

1. Vorrichtung (10) zum Erzeugen eines verschlüsselten Datenstroms aus einem Audiosignal, mit folgenden Merkmalen:

einem Codierer (16) zum Codieren des Audiosignals, um als Ausgangssignal einen Datenstrom mit einer vordefinierten Datenstromsyntax zu erzeugen;

einer Verschlüsselungseinrichtung (18), die mit dem Codierer (16) gekoppelt ist, zum Beeinflussen von codiererinternen Daten (20a) auf eine eindeutig umkehrbare Art und Weise auf der Basis eines Schlüssels (k1), derart, daß der erzeugte verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines Datenstroms unterscheiden, der durch die Vorrichtung (10) ohne Vorhandensein der Verschlüsselungseinrichtung (18) erzeugt werden würde, und daß der erzeugte verschlüsselte Datenstrom die vordefinierte Datenstromsyntax aufweist,

wobei der Codierer ein Codierer für Audiosignale ist, der folgende Merkmale aufweist:

eine Analysefilterbank (204) zum Umsetzen des Audiosignals von dem Zeitbereich in eine spektrale Darstellung, um Spektralwerte zu erhalten;

eine Quantisierungseinrichtung (206) zum Quantisieren der Spektralwerte unter Berücksichtigung eines psychoakustischen Modells (208); und

einen Entropie-Codierer (210), der angeordnet ist, um eine Entropie-Codierung der quantisierten Spektralwerte mittels einer Mehrzahl von vordefinierten Codetabellen durchzuführen, wobei jede Codetabelle für die Entropiecodierung von quantisierten Spek-

tralwerten in einem Frequenzband vorgesehen ist, und wobei zumindest ein Frequenzband zwei oder mehrere quantisierte Spektralwerte aufweist, und

wobei die Verschlüsselungseinrichtung (18) angeordnet ist, um basierend auf dem Schlüssel die zwei oder mehr quantisierten Spektralwerte in dem Frequenzband, das zwei oder mehr quantisierte Spektralwerte aufweist, und dem eine Codetabelle zugeordnet ist, umzusortieren.

2. Vorrichtung nach Anspruch 1, bei der die Verschlüsselungseinrichtung (18) ferner angeordnet ist, um auf der Basis des Schlüssels die zwei oder mehr quantisierten Spektralwerte so umzusortieren, daß der verschlüsselte Datenstrom die gleiche Länge in Bit hat wie ein Datenstrom, der durch die Vorrichtung (10) ohne Vorhandensein der Verschlüsselungseinrichtung erzeugt werden würde.
3. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der die Verschlüsselungseinrichtung (18) angeordnet ist, um auf der Basis des Schlüssels die zwei oder mehr quantisierten Spektralwerte lediglich so umzusortieren, daß sich die Nutzinformationen des verschlüsselten Datenstroms nur so stark von den Nutzinformationen eines Datenstroms unterscheiden, der ohne Vorhandensein der Verschlüsselungseinrichtung (18) erzeugt werden würde, daß ein Decodierer, der nicht im Besitz des Schlüssels ist, aufgrund der verschlüsselten Daten ein decodiertes Ausgangssignal mit einer Qualität liefert, die geringer als die Qualität ist, die der Decodierer liefern würde, wenn er im Besitz des Schlüssels wäre, wobei jedoch eine Mindestqualität sichergestellt ist.
4. Vorrichtung nach einem der Ansprüche 1 bis 3, bei der die Quantisierungseinrichtung (206) angeordnet ist, um die quantisierten Spektralwerte als Hauptinformationen

und Skalenfaktoren, von denen jeder mindestens einem quantisierten Spektralwert zugeordnet ist, als Seiteninformationen zu erzeugen; und

wobei die Verschlüsselungseinrichtung (18) ferner angeordnet ist, um die durch die Quantisierungseinrichtung (206) erzeugten Skalenfaktoren auf der Basis des Schlüssels zu beeinflussen.

5. Vorrichtung nach Anspruch 1, bei der die Verschlüsselungseinrichtung angeordnet ist, um die quantisierten Spektralwerte in dem Frequenzband, das zwei oder mehrere Spektralwerte aufweist, mit einer Pseudo-Zufallsbitfolge, die aufgrund des Schlüssels als Startwert erzeugt wird, mittels einer EXKLUSIV-ODER-Verknüpfung zu verknüpfen.
6. Vorrichtung nach Anspruch 1, bei der ferner lediglich niederwertige Bits von Spektralwerten mit einer Pseudo-Zufallsbitfolge verknüpft werden.
7. Vorrichtung nach Anspruch 1, bei der die quantisierten Spektralwerte vorzeichenbehaftet sind, und bei der die Verschlüsselungseinrichtung (18) ferner angeordnet ist, um auf der Basis des Schlüssels Vorzeichen von quantisierten Spektralwerten zu verändern.
8. Vorrichtung nach Anspruch 1, bei der der Entropie-Codierer (210) derart angeordnet ist, daß er zumindest eine Codetabelle aufweist, die eine vorzeichenlose Codetabelle ist, derart, daß ein Vorzeichen für ein Codewort aus der Codetabelle getrennt von dem Codewort in die Nutzinformationen geschrieben wird, wobei die Verschlüsselungseinrichtung (18) ferner angeordnet ist, um vor der Entropie-Codierung der quantisierten Spektralwerte das Vorzeichen zumindest eines quantisierten Spektralwerts basierend auf dem Schlüssel zu verändern.

9. Vorrichtung nach Anspruch 1, bei der zumindest eine Codetabelle der Mehrzahl von Codetabellen eine mehrdimensionale Codetabelle ist, bei der ein Codewort eine Mehrzahl von quantisierten Spektralwerten darstellt, wobei die Verschlüsselungseinrichtung (18) angeordnet ist, um Gruppen von quantisierten Spektralwerten umzusortieren, wobei eine Gruppe von Spektralwerten so viele quantisierte Spektralwerte aufweist, wie sie durch ein Codewort der mehrdimensionalen Codetabelle codiert werden.
10. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der der Codierer eine Mehrzahl von Unterblöcken (204 bis 210) aufweist, die mit einem Bitstrommultiplexer (212) verbunden sind, der von den einzelnen Unterblöcken ausgegebene Daten gemäß der vordefinierten Datenstromsyntax multiplext, um die Ausgangsdaten des Codierers (16) zu erhalten.
11. Vorrichtung (70) zum Erzeugen eines auf der Basis eines zweiten Schlüssels (k_2) verschlüsselten zweiten Datenstroms aus einem auf der Basis eines ersten Schlüssels (k_1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß zwei oder mehr quantisierten Spektralwerte in einem Frequenzband, das zwei oder mehr quantisierte Spektralwerte aufweist, und dem eine Codetabelle zugeordnet ist, auf der Basis des ersten Schlüssels umsortiert worden sind, wobei nach der Umsortierung eine Entropie-Codierung der quantisierten Spektralwerte mittels einer Mehrzahl von vordefinierten Codetabellen durchgeführt wurde, wobei jede Codetabelle für die Entropiecodierung von quantisierten Spektralwerten in einem Frequenzband vorgesehen ist, und wobei zumindest ein Frequenzband die zwei oder mehreren quantisierte Spektralwerte aufweist, mit folgenden Merkma-

len:

einem Teil-Decodierer (36') zum Rückgängigmachen eines Teils der Codierung, derart, daß die umsortierten zwei oder mehreren Spektralwerte vorliegen;

einer Entschlüsselungseinrichtung (38) zum Entschlüsseln der umsortierten zwei oder mehreren Spektralwerte durch Rückgängigmachen der Umsortierung auf der Basis des ersten Schlüssels (k1);

einer Verschlüsselungseinrichtung (18) zum Beeinflussen der Reihenfolge der zwei oder mehreren Spektralwerte des Frequenzbands, dem eine Codetabelle zugeordnet ist, auf der Basis des zweiten Schlüssels (k2);

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den auf der Basis des zweiten Schlüssels (k2) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

12. Vorrichtung (70') zum Erzeugen eines auf der Basis eines Schlüssels (k1) verschlüsselten zweiten Datenstroms aus einem ersten Datenstrom, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, mit folgenden Merkmalen:

einem Teil-Decodierer (36') zum Rückgängigmachen eines Teils der Codierung, derart, daß quantisierte Spektralwerte des Audiosignals vorliegen;

einer Verschlüsselungseinrichtung (18) zum Umsortieren von zwei oder mehr quantisierten Spektralwerten in einem Frequenzband, das zwei oder mehr quantisierte Spektralwerte aufweist, auf der Basis des ersten

Schlüssels (k1), wobei dem Frequenzband eine einer Mehrzahl von vordefinierten Codetabellen für eine Entropie-Codierung zugeordnet ist, wobei jede Codetabelle für die Entropiecodierung von quantisierten Spektralwerten in einem Frequenzband vorgesehen ist, und wobei zumindest ein Frequenzband die zwei oder mehreren quantisierte Spektralwerte aufweist, wobei die Verschlüsselungseinrichtung angeordnet ist, um die quantisierten Spektralwerte eines Frequenzbands umzusortieren, denen dieselbe Codetabelle zugeordnet ist;

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den auf der Basis des Schlüssels (k1) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

13. Vorrichtung (80) zum Erzeugen eines entschlüsselten Datenstroms aus einem auf der Basis eines Schlüssels (k1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß zumindest zwei oder mehr quantisierte Spektralwerte in einem Frequenzband auf der Basis des ersten Schlüssels (k1) umsortiert worden sind, wobei dem Frequenzband, dessen quantisierte Spektralwerte umsortiert worden sind, eine einer Mehrzahl von vordefinierten Codetabellen für eine Entropie-Codierung zugeordnet ist, wobei jede Codetabelle für die Entropiecodierung von quantisierten Spektralwerten in einem Frequenzband vorgesehen ist, und wobei zumindest ein Frequenzband die zwei oder mehreren quantisierte Spektralwerte aufweist, mit folgenden Merkmalen:

einem Teil-Decodierer (36') zum Rückgängigmachen eines Teils der Codierung, derart, daß die umsortierten zwei

oder mehreren quantisierten Spektralwerte vorliegen, wobei die umsortierten zwei oder mehreren quantisierten Spektralwerte zu einem Frequenzband gehören, dem eine Codetabelle zugeordnet ist;

einer Entschlüsselungseinrichtung (38) zum Entschlüsseln der umsortierten zwei oder mehreren quantisierten Spektralwerte durch Rückgängigmachen der Umsortierung auf der Basis des Schlüssels (k1);

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den zweiten Datenstrom mit der vordefinierten Datenstromsyntax zu erzeugen.

14. Vorrichtung nach einem der Ansprüche 11 bis 13,

bei der der Teil-Decodierer (36') einen Bitstrom-Demultiplexer (222) aufweist, wobei die codiererinternen Daten die Ausgangsdaten aus dem Bitstrom-Demultiplexer (222) sind.

15. Vorrichtung nach Anspruch 19,

bei der der Teil-Decodierer (36') ferner einen dem Bitstrom-Demultiplexer (222) nachgeschalteten Entropie-Decodierer (224) aufweist, wobei die codiererinternen Daten die Ausgangsdaten aus dem Entropie-Decodierer (224) sind.

16. Vorrichtung nach einem der Ansprüche 17 bis 19, bei der neben den zwei oder mehreren quantisierten Spektralwerten auch Skalenfaktoren beeinflußt werden.

17. Vorrichtung (30) zum Erzeugen eines entschlüsselten Audiosignals aus einem verschlüsselten Datenstrom, der ein auf eindeutig umkehrbare Art und Weise innerhalb eines Frequenzbandes umsortierte quantisierte und an-

schließlich Entropie-codierte Spektralwerte eines Audio-signals aufweist, wobei das Frequenzband dadurch definiert ist, daß ihm eine Codetabelle aus einer Mehrzahl von Codetabellen für die Entropie-Codierung zugeordnet ist, wobei der verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines unverschlüsselten Datenstroms unterscheiden, und wobei der verschlüsselte Datenstrom dieselbe Datenstromsyntax wie ein unverschlüsselter Datenstrom aufweist, mit folgenden Merkmalen:

einem Decodierer (36) zum Decodieren von Eingangsdaten, um decodierte Ausgangsdaten zu erzeugen, wobei der Decodierer einen Entropie-Decodierer (24) zum Rückgängigmachen der Entropie-Codierung aufweist, um die umsortierten quantisierten Spektralwerte zu erhalten; und

einer Entschlüsselungseinrichtung (38) zum Beeinflussen der umsortierten quantisierten Spektralwerte auf der Basis eines Schlüssels, um die eindeutig umkehrbare Umsortierung, die in einer Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms durchgeführt worden ist, rückgängig zu machen, um das entschlüsselte Audio-signal zu erhalten.

18. Vorrichtung (30) nach Anspruch 17, bei der der Decodierer ferner folgende Merkmale aufweist:

eine Mehrzahl von Funktionsblöcken, die mit einem Bitstrom-Demultiplexer (222) gekoppelt sind, der Teile des Datenstroms gemäß der vordefinierten Datenstromsyntax zu den einzelnen Blöcken leitet.

19. Vorrichtung (30) nach einem der Ansprüche 18 oder 19, bei der der Decodierer (36) ferner folgendes Merkmal aufweist:

eine Synthesefilterbank (228), um eine spektrale Dar-

stellung des Audiosignals in eine zeitliche Darstellung umzusetzen.

20. Verfahren (10) zum Erzeugen eines verschlüsselten Datenstroms aus einem Audiosignal, mit folgenden Schritten:

Codieren (16) des Audiosignals, um als Ausgangssignal einen Datenstrom mit einer vordefinierten Datenstromsyntax zu erzeugen;

Verschlüsseln von codiererinternen Daten (20a) durch Beeinflussen (18) derselben auf eine eindeutig umkehrbare Art und Weise auf der Basis eines Schlüssels (k1), derart, daß der erzeugte verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines Datenstroms unterscheiden, der ohne den Schritt des Verschlüsseln erzeugt werden würde, und daß der erzeugte verschlüsselte Datenstrom die vordefinierte Datenstromsyntax aufweist,

wobei im Schritt des Codierens ein Audiosignal codiert wird, mit folgenden Schritten:

Umsetzen (204) des Audiosignals von dem Zeitbereich in eine spektrale Darstellung, um Spektralwerte zu erhalten;

Quantisieren (206) der Spektralwerte unter Berücksichtigung eines psychoakustischen Modells (208); und

Entropie-Codieren (210) der quantisierten Spektralwerte mittels einer Mehrzahl von vordefinierten Codetabellen durchzuführen, wobei jede Codetabelle für die Entropiecodierung von quantisierten Spektralwerten in einem Frequenzband vorgesehen ist, und wobei zumindest ein Frequenzband zwei oder mehrere

quantisierte Spektralwerte aufweist, und

wobei der Schritt des Verschlüsseln (18) ausgeführt wird, um basierend auf dem Schlüssel die zwei oder mehr quantisierten Spektralwerte in dem Frequenzband, das zwei oder mehr quantisierte Spektralwerte aufweist, und dem eine Codetabelle zugeordnet ist, umzusortieren.

21. Verfahren (70) zum Erzeugen eines auf der Basis eines zweiten Schlüssels (k_2) verschlüsselten zweiten Datenstroms aus einem auf der Basis eines ersten Schlüssels (k_1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß zwei oder mehr quantisierten Spektralwerte in einem Frequenzband, das zwei oder mehr quantisierte Spektralwerte aufweist, und dem eine Codetabelle zugeordnet ist, auf der Basis des ersten Schlüssels umsortiert worden sind, wobei nach der Umsortierung eine Entropie-Codierung der quantisierten Spektralwerte mittels einer Mehrzahl von vordefinierten Codetabellen durchgeführt wurde, wobei jede Codetabelle für die Entropiecodierung von quantisierten Spektralwerten in einem Frequenzband vorgesehen ist, und wobei zumindest ein Frequenzband die zwei oder mehreren quantisierte Spektralwerte aufweist, mit folgenden Schritten:

Rückgängigmachen (36') eines Teils der Codierung, derart, daß die umsortierten zwei oder mehreren Spektralwerte vorliegen;

Entschlüsseln (38) der umsortierten zwei oder mehreren Spektralwerte durch Rückgängigmachen der Umsortierung auf der Basis des ersten Schlüssels (k_1);

Verschlüsseln (18) durch Beeinflussen der Reihenfolge der zwei oder mehreren Spektralwerte des Frequenzbands, dem eine Codetabelle zugeordnet ist, auf der Basis des zweiten Schlüssels (k_2);

Durchführen (16') des Teils der Codierung, der durch den Schritt des Rückgängigmachens (36') rückgängig gemacht worden ist, um den auf der Basis des zweiten Schlüssels (k_2) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

22. Verfahren (70') zum Erzeugen eines auf der Basis eines Schlüssels (k_1) verschlüsselten zweiten Datenstroms aus einem ersten Datenstrom, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, mit folgenden Schritten:

Rückgängigmachen (36') eines Teils der Codierung, derart, daß quantisierte Spektralwerte des Audiosignals vorliegen;

Verschlüsseln (18) durch Umsortieren von zwei oder mehr quantisierten Spektralwerten in einem Frequenzband, das zwei oder mehr quantisierte Spektralwerte aufweist, auf der Basis des ersten Schlüssels (k_1), wobei dem Frequenzband eine einer Mehrzahl von vordefinierten Codetabellen für eine Entropie-Codierung zugeordnet ist, wobei jede Codetabelle für die Entropiecodierung von quantisierten Spektralwerten in einem Frequenzband vorgesehen ist, und wobei zumindest ein Frequenzband die zwei oder mehreren quantisierte Spektralwerte aufweist, wobei die Verschlüsselungseinrichtung angeordnet ist, um die quantisierten Spektralwerte eines Frequenzbands umzusortieren, denen dieselbe Codetabelle zugeordnet ist;

Durchführen (16') des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den auf der Basis des Schlüssels (k1) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

23. Verfahren (80) zum Erzeugen eines entschlüsselten Datenstroms aus einem auf der Basis eines Schlüssels (k1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß zumindest zwei oder mehr quantisierte Spektralwerte in einem Frequenzband auf der Basis des ersten Schlüssels (k1) umsortiert worden sind, wobei dem Frequenzband, dessen quantisierte Spektralwerte umsortiert worden sind, eine einer Mehrzahl von vordefinierten Codetabellen für eine Entropie-Codierung zugeordnet ist, wobei jede Codetabelle für die Entropiecodierung von quantisierten Spektralwerten in einem Frequenzband vorgesehen ist, und wobei zumindest ein Frequenzband die zwei oder mehreren quantisierte Spektralwerte aufweist, mit folgenden Schritten:

Rückgängigmachen (36') eines Teils der Codierung, derart, daß die umsortierten zwei oder mehreren quantisierten Spektralwerte vorliegen, wobei die umsortierten zwei oder mehreren quantisierten Spektralwerte zu einem Frequenzband gehören, dem eine Codetabelle zugeordnet ist;

Entschlüsseln (38) der umsortierten zwei oder mehreren quantisierten Spektralwerte durch Rückgängigmachen der Umsortierung auf der Basis des Schlüssels (k1);

Durchführen (16') des Teils der Codierung, der durch den Schritt des Rückgängigmachens (36') rückgängig gemacht worden ist, um den zweiten Datenstrom mit der

vordefinierten Datenstromsyntax zu erzeugen.

24. Verfahren (30) zum Erzeugen eines entschlüsselten Audiosignals aus einem verschlüsselten Datenstrom, der ein auf eindeutig umkehrbare Art und Weise innerhalb eines Frequenzbandes umsortierte quantisierte und anschließend Entropie-codierte Spektralwerte eines Audiosignals aufweist, wobei das Frequenzband dadurch definiert ist, daß ihm eine Codetabelle aus einer Mehrzahl von Codetabellen für die Entropie-Codierung zugeordnet ist, wobei der verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines unverschlüsselten Datenstroms unterscheiden, und wobei der verschlüsselte Datenstrom dieselbe Datenstromsyntax wie ein unverschlüsselter Datenstrom aufweist, mit folgenden Schritten:

Decodieren (36) von Eingangsdaten, um decodierte Ausgangsdaten zu erzeugen, wobei im Schritt des Decodierens ein Entropie-Decodieren (24) zum Rückgängigmachen der Entropie-Codierung durchgeführt wird, um die umsortierten quantisierten Spektralwerte zu erhalten; und

Entschlüsseln (38) durch Beeinflussen der umsortierten quantisierten Spektralwerte auf der Basis eines Schlüssels, um die eindeutig umkehrbare Umsortierung, die bei einem Erzeugen eines verschlüsselten Datenstroms durchgeführt worden ist, rückgängig zu machen, um das entschlüsselte Audiosignal zu erhalten.

25. Vorrichtung (10) zum Erzeugen eines verschlüsselten Datenstroms aus einem Audiosignal, mit folgenden Merkmalen:

einem Codierer (16) zum Codieren des Audiosignals, um als Ausgangssignal einen Datenstrom mit einer vordefinierten Datenstromsyntax zu erzeugen;

einer Verschlüsselungseinrichtung (18), die mit dem Codierer (16) gekoppelt ist, zum Beeinflussen von codiererinternen Daten (20a) des Codierers (16) auf eine eindeutig umkehrbare Art und Weise auf der Basis eines Schlüssels (k1), derart, daß der erzeugte verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines Datenstroms unterscheiden, der durch die Vorrichtung (10) ohne Vorhandensein der Verschlüsselungseinrichtung (18) erzeugt werden würde, und daß der erzeugte verschlüsselte Datenstrom die vordefinierte Datenstromsyntax aufweist,

wobei der Codierer (16) ein Codierer für Audiosignale ist, der folgende Merkmale aufweist:

eine Analysefilterbank (204) zum Umsetzen des Audiosignals von dem Zeitbereich in eine spektrale Darstellung, um Spektralwerte zu erhalten;

eine Quantisierungseinrichtung (206) zum Quantisieren der Spektralwerte unter Berücksichtigung eines psychoakustischen Modells (208); und

einen Entropie-Codierer (210), der angeordnet ist, um eine Entropie-Codierung der quantisierten Spektralwerte durchzuführen, um eine Folge von Codewörtern zu erhalten, wobei die Folge von Codewörtern eine entropiecodierte Version des Audiosignals darstellt, und

wobei die Verschlüsselungseinrichtung (18) angeordnet ist, um basierend auf dem Schlüssel die Folge von Codewörtern durch Ändern einer Reihenfolge der Codewörter umzusortieren.

26. Vorrichtung nach Anspruch 25, bei der die Verschlüsselungseinrichtung (18) angeordnet ist, um auf der Basis des Schlüssels die Codewörter lediglich so stark umzusortieren, daß sich die Nutzinformationen des verschlüsselten Datenstroms nur so stark von den Nutzinformationen eines Datenstroms unterscheiden, der ohne Vorhandensein der Verschlüsselungseinrichtung (18) erzeugt werden würde, daß ein Decodierer, der nicht im Besitz des Schlüssels ist, aufgrund der verschlüsselten Daten ein decodiertes Ausgangssignal mit einer Qualität liefert, die geringer als die Qualität ist, die der Decodierer liefern würde, wenn er im Besitz des Schlüssels wäre, wobei jedoch eine Mindestqualität sichergestellt ist.
27. Vorrichtung nach Anspruch 25 oder 26, bei der immer zwei benachbarte Codewörter miteinander vertauscht werden.
28. Vorrichtung (70) zum Erzeugen eines auf der Basis eines zweiten Schlüssels (k_2) verschlüsselten Datenstroms aus einem auf der Basis eines ersten Schlüssels (k_1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß basierend auf dem ersten Schlüssel (k_1) eine Folge von Codewörtern, die durch Entropie-Codierung von quantisierten Spektralwerten erzeugt wurden, durch Ändern einer Reihenfolge der Codewörter umsortiert worden sind, mit folgenden Merkmalen:

einem Teil-Decodierer (36') zum Rückgängigmachen eines

Teils der Codierung, derart, daß die umsortierte Folge von Codewörtern vorliegt;

einer Entschlüsselungseinrichtung (38) zum Rückgängigmachen der Umsortierung auf der Basis des ersten Schlüssels (k1);

einer Verschlüsselungseinrichtung (18) zum Umsortieren der Folge von Codewörtern auf der Basis des zweiten Schlüssels (k2) durch Ändern einer Reihenfolge der Codewörter;

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den auf der Basis des zweiten Schlüssels (k2) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

29. Vorrichtung (70') zum Erzeugen eines auf der Basis eines Schlüssels (k1) verschlüsselten zweiten Datenstroms aus einem ersten Datenstrom, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, mit folgenden Merkmalen:

einem Teil-Decodierer (36') zum Rückgängigmachen eines Teils der Codierung, derart, daß eine Folge von Codewörtern, die durch Entropie-Codierung von quantisierten Spektralwerten erzeugt wurden, vorliegt;

einer Verschlüsselungseinrichtung (18) zum Umsortieren der Folge von Codewörtern auf der Basis des Schlüssels (k1) durch Ändern einer Reihenfolge der Codewörter;

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den auf der Basis des

Schlüssels (k1) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

30. Vorrichtung (80) zum Erzeugen eines entschlüsselten Datenstroms aus einem auf der Basis eines Schlüssels (k1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß basierend auf dem ersten Schlüssel (k1) eine Folge von Codewörtern, die durch Entropie-Codierung von quantisierten Spektralwerten erzeugt wurden, durch Ändern einer Reihenfolge der Codewörter umsortiert worden ist, mit folgenden Merkmalen:

einem Teil-Decodierer (36') zum Rückgängigmachen eines Teils der Codierung, derart, daß die umsortierte Folge von Codewörtern vorliegt;

einer Entschlüsselungseinrichtung (38) zum Rückgängigmachen der Umsortierung der Folge von Codewörtern auf der Basis des Schlüssels (k1);

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den zweiten Datenstrom mit der vordefinierten Datenstromsyntax zu erzeugen.

31. Vorrichtung (30) zum Erzeugen eines entschlüsselten Audiosignals aus einem verschlüsselten Datenstrom, der eine auf eindeutig umkehrbare Weise durch Ändern einer Reihenfolge der Codewörter umsortierte Folge von Codewörtern, die durch Entropie-Codierung von quantisierten Spektralwerten erzeugt wurden, aufweist, wobei der verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines unverschlüsselten Datenstroms unterscheiden, und wobei der verschlüsselte

Datenstrom dieselbe Datenstromsyntax wie ein unverschlüsselter Datenstrom aufweist, mit folgenden Merkmalen:

einem Decodierer (36) zum Decodieren von Eingangsdaten, um decodierte Ausgangsdaten zu erzeugen; und

einer Entschlüsselungseinrichtung (38) zum Beeinflussen der umsortierten Folge von Codewörtern auf der Basis eines Schlüssels, um die Umsortierung, die in einer Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms durchgeführt worden ist, rückgängig zu machen, um das entschlüsselte Audiosignal zu erhalten.

32. Verfahren (10) zum Erzeugen eines verschlüsselten Datenstroms aus einem Audiosignal, mit folgenden Schritten:

Codieren (16) des Audiosignals, um als Ausgangssignal einen Datenstrom mit einer vordefinierten Datenstromsyntax zu erzeugen;

Verschlüsseln (18) durch Beeinflussen von codiererinternen Daten (20a) im Schritt des Codierens (16) auf eine eindeutig umkehrbare Art und Weise auf der Basis eines Schlüssels (k_1), derart, daß der erzeugte verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines Datenstroms unterscheiden, der durch die Vorrichtung (10) ohne Vorhandensein der Verschlüsselungseinrichtung (18) erzeugt werden würde, und daß der erzeugte verschlüsselte Datenstrom die vordefinierte Datenstromsyntax aufweist,

wobei der Schritt des Codierens (16) folgende Schritte aufweist:

Umsetzen (204) des Audiosignals von dem Zeitbereich in eine spektrale Darstellung, um Spektralwerte zu

erhalten;

Quantisieren (206) der Spektralwerte unter Berücksichtigung eines psychoakustischen Modells (208);
und

Entropie-Codieren (210) der quantisierten Spektralwerte, um eine Folge von Codewörtern zu erhalten, wobei die Folge von Codewörtern eine entropiecodierte Version des Audiosignals darstellt, und

wobei im Schritt des Verschlüsseln (18), basierend auf dem Schlüssel, durch Ändern einer Reihenfolge der Codewörter die Folge von Codewörtern umsortiert wird.

33. Verfahren (70) zum Erzeugen eines auf der Basis eines zweiten Schlüssels (k2) verschlüsselten Datenstroms aus einem auf der Basis eines ersten Schlüssels (k1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß basierend auf dem ersten Schlüssel (k1) eine Folge von Codewörtern, die durch Entropie-Codierung von quantisierten Spektralwerten erzeugt wurden, durch Ändern einer Reihenfolge der Codewörter umsortiert worden sind, mit folgenden Merkmalen:

Rückgängigmachen (36y) eines Teils der Codierung, derart, daß die umsortierte Folge von Codewörtern vorliegt;

Rückgängigmachen (38) der Umsortierung auf der Basis des ersten Schlüssels (k1);

Verschlüsseln (18) durch Umsortieren der Folge von Codewörtern auf der Basis des zweiten Schlüssels (k2);

Durchführen (16'') des Teils der Codierung, der im Schritt des Rückgängigmachens (36') rückgängig gemacht worden ist, um den auf der Basis des zweiten Schlüssels (k2) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

34. Verfahren (70') zum Erzeugen eines auf der Basis eines Schlüssels (k1) verschlüsselten zweiten Datenstroms aus einem ersten Datenstrom, wobei der erste Datenstrom ein codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, mit folgenden Schritten:

Rückgängigmachen (36'') eines Teils der Codierung, derart, daß eine Folge von Codewörtern, die durch Entropie-Codierung von quantisierten Spektralwerten erzeugt wurden, vorliegt;

Verschlüsseln (18) durch Umsortieren der Folge von Codewörtern auf der Basis des Schlüssels (k1) durch Ändern einer Reihenfolge der Codewörter;

Durchführen (16'') des Teils der Codierung, der durch den Schritt des Rückgängigmachens (36') rückgängig gemacht worden ist, um den auf der Basis des Schlüssels (k1) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

35. Verfahren (80) zum Erzeugen eines entschlüsselten Datenstroms aus einem auf der Basis eines Schlüssels (k1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein codiertes Audiosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß basierend auf dem ersten Schlüssel (k1) eine Folge von Codewörtern, die durch Entropie-Codierung von quantisierten Spektralwerten erzeugt wurden, durch Ändern einer Reihenfolge der

Codewörter umsortiert worden ist, mit folgenden Merkmalen:

Rückgängigmachen (36 \ddot{y}) eines Teils der Codierung, derart, daß die umsortierte Folge von Codewörtern vorliegt;

Entschlüsseln (38) durch Rückgängigmachen der Umsortierung der Folge von Codewörtern auf der Basis des Schlüssels (k1);

Durchführen (16 \ddot{y}) des Teils der Codierung, der durch den Schritt des Rückgängigmachens (36') rückgängig gemacht worden ist, um den zweiten Datenstrom mit der vordefinierten Datenstromsyntax zu erzeugen.

36. Verfahren (30) zum Erzeugen eines entschlüsselten Audiosignals aus einem verschlüsselten Datenstrom, der eine durch Ändern einer Reihenfolge der Codewörter auf eindeutig umkehrbare Weise umsortierte Folge von Codewörtern, die durch Entropie-Codierung von quantisierten Spektralwerten erzeugt wurden, aufweist, wobei der verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines unverschlüsselten Datenstroms unterscheiden, und wobei der verschlüsselte Datenstrom dieselbe Datenstromsyntax wie ein unverschlüsselter Datenstrom aufweist, mit folgenden Schritten:

Decodieren (36) von Eingangsdaten, um decodierte Ausgangsdaten zu erzeugen; und

Entschlüsseln (38) durch Beeinflussen der umsortierten Folge von Codewörtern auf der Basis eines Schlüssels, um die Umsortierung, die beim Erzeugen eines verschlüsselten Datenstroms durchgeführt worden ist, rückgängig zu machen, um das entschlüsselte Audiosignal zu erhalten.

Translation
09/9/4 371

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference FH991205PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP99/09978	International filing date (day/month/year) 15 December 1999 (15.12.99)	Priority date (day/month/year) 24 February 1999 (24.02.99)
International Patent Classification (IPC) or national classification and IPC H04K 1/00, H04N 7/167, 7/26		
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E. V.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.	
2. This REPORT consists of a total of <u>10</u> sheets, including this cover sheet.	
<input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).	
These annexes consist of a total of <u>24</u> sheets.	
3. This report contains indications relating to the following items:	
I <input checked="" type="checkbox"/>	Basis of the report
II <input type="checkbox"/>	Priority
III <input type="checkbox"/>	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
IV <input checked="" type="checkbox"/>	Lack of unity of invention
V <input checked="" type="checkbox"/>	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
VI <input type="checkbox"/>	Certain documents cited
VII <input checked="" type="checkbox"/>	Certain defects in the international application
VIII <input type="checkbox"/>	Certain observations on the international application

Date of submission of the demand 22 September 2000 (22.09.00)	Date of completion of this report 29 June 2001 (29.06.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP99/09978

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

- ☐ the international application as originally filed.
- ☒ the description, pages 1, 2, 4-24, as originally filed,
 pages _____, filed with the demand,
 pages 3, 3a-3b, filed with the letter of 07 June 2001 (07.06.2001),
 pages _____, filed with the letter of _____.
- ☒ the claims, Nos. _____, as originally filed,
 Nos. _____, as amended under Article 19,
 Nos. _____, filed with the demand,
 Nos. 1-36, filed with the letter of 07 June 2001 (07.06.2001),
 Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 1/8-8/8, as originally filed,
 sheets/fig _____, filed with the demand,
 sheets/fig _____, filed with the letter of _____,
 sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP99/09978

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

- ☐ restricted the claims.
- ☐ paid additional fees.
- ☐ paid additional fees under protest.
- ☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

- ☐ complied with.
- ☒ not complied with for the following reasons:

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

- ☒ all parts.
- ☐ the parts relating to claims Nos. _____

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: IV

1. Cited document:

D1 = QUACKENBUSH ET AL.: 'Noiseless Coding of Quantized Spectral Components in MPEG-2 Advanced Audio Coding' 1997 IEEE ASSP WORKSHOP ON APPLICATIONS OF SIGNAL PROCESSING TO AUDIO AND ACOUSTICS, 19 October 1997 (1997-10-19).

2. The various groups of inventions are: Claims 1 to 24 and 25 to 36.

These groups are not so linked as to form a single general inventive concept for the following reasons (PCT Rule 13.1):

D1 describes (see Figure 1) a device for encoding a data stream from an audio signal, comprising the features of the encoder defined in the claims.

The first group additionally claims an encryption of the signal by means of resorting the quantized spectral values and the second group additionally claims an encryption by means of resorting code words.

The technical relationship between the first and the second group lies in the features of the encoder. These features are known from D1.

No technical relationship within the meaning of PCT Rule 13.2 exists between the features of the

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: IV

encryption in the first and in the second group.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-36	YES
	Claims		NO
Inventive step (IS)	Claims	1-24	YES
	Claims	25-36	NO
Industrial applicability (IA)	Claims	1-36	YES
	Claims		NO

2. Citations and explanations

1. Cited documents:

D1 = QUACKENBUSH ET AL.: 'Noiseless Coding of Quantized Spectral Components in MPEG-2 Advanced Audio Coding' 1997 IEEE ASSP WORKSHOP ON APPLICATIONS OF SIGNAL PROCESSING TO AUDIO AND ACOUSTICS, 19 October 1997 (1997-10-19)

D2 = US-A-5 796 838

D3 = US-A-4 534 037

D4 = EP-A-0 649 261

D5 = WO98/21852

D6 = US-A-5 636 279.

2. The subject matter of Claim 1 is novel and inventive in relation to the prior art cited in the international search report. Claim 1 therefore meets the requirements of PCT Article 33(2) and (3).

D1 describes (see Figure 1) a device for encoding a data stream from an audio signal, comprising the features of the encoder defined in the claims.

D2 describes a spectral inversion in which the output spectrum is inverted in relation to the input spectrum. The shape of the spectrum is only reflected by the frequency inversion, but not completely changed, as would be the case with scrambling.

None of the documents cited in the search report suggests the resorting of quantized spectral values in a frequency band to which one code table of a plurality of code tables is allocated.

By means of the aforementioned resorting process, a "soft" encryption is achieved which does not change the data stream syntax of the encoder.

The subject matter of Claim 1 is therefore novel and inventive in relation to the prior art cited in the search report.

3. The subject matter of Claims 2 to 10 is novel and inventive in relation to the prior art cited in the international search report. Claims 2 to 10 therefore meet the requirements of PCT Article 33(2) and (3).

Claims 2 to 10 are either directly or indirectly dependent on Claim 1.

4. The subject matter of Claims 11 to 13 is novel and inventive in relation to the prior art cited in the international search report. Claims 11 to 13 therefore meet the requirements of PCT Article 33(2)

and (3).

The subject matter of Claims 11 to 13 differs from the subject matter of Claim 1 in that former claims have additional means for canceling the encryption on the basis of a first code and for carrying out an encryption on the basis of a second code.

The subject matter of Claims 11 to 13 is therefore novel and inventive for the reasons mentioned under point 2.

5. The subject matter of Claims 14, 15 and 16 is novel and inventive in relation to the prior art cited in the international search report. Claims 14, 15 and 16 meet the requirements of PCT Article 33(2) and (3).

Claims 14, 15 and 16 are either directly or indirectly dependent on Claims 11 to 13.

6. The subject matter of Claims 17 to 19 is novel and inventive in relation to the prior art cited in the international search report. Claims 17 to 19 therefore meet the requirements of PCT Article 33(2) and (3).

Claims 17 to 19 relate to a device for decoding a data stream, wherein the resorting process defined in Claim 1 is cancelled.

The subject matter of Claims 17 to 19 is therefore novel and inventive for the reasons mentioned under point 2.

7. The subject matter of Claims 20 to 24 is novel and inventive in relation to the prior art cited in the international search report. Claims 20 to 24 therefore meet the requirements of PCT Article 33(2) and (3).

Claims 20 to 24 define a method with method steps which correspond to the features of the previously claimed device.

The subject matter of Claims 20 to 24 is therefore novel and inventive for the reasons mentioned under point 2.

8. The subject matter of Claim 25 is not inventive in relation to the content of D1 and D3. Claim 25 therefore does not meet the requirements of PCT Article 33(3).

D1 describes (see Figure 1) a device for encoding a data stream from an audio signal, comprising the features of the encoder defined in the claims.

D3 describes an encryption of audio signals by means of resorting bit groups between neighboring code words. If the frequency conversion described in D3 (see column 4, lines 56-61) is not the aim, it would be obvious to a person skilled in the art to carry out the encryption by resorting code words. Thus the encryption of an audio signal by resorting code words is obvious from D3.

A person skilled in the art would inevitably attempt to combine the encoding known from D1 with the encryption which is obvious from D3.

9. The subject matter of Claims 26 and 27 is not inventive in relation to the content of D1 and D3. Claims 26 and 27 therefore do not meet the requirements of PCT Article 33(3).

The additional feature of Claim 26 relates to a feature of an encrypting device with which a person skilled in the art is familiar.

The additional feature of Claim 27 is known from D3.

10. The subject matter of Claims 28 and 29 is not inventive in relation to the content of D1, D3 and D5. Claims 28 and 29 therefore do not meet the requirements of PCT Article 33(3).

The subject matter of Claims 28 and 29 differs from the subject matter of Claim 25 in that the former claims have additional means for canceling the encryption on the basis of a first code and for carrying out an encryption on the basis of a second code.

The transition from a first code to a second code is known from D5. A person skilled in the art would incorporate this feature into the claimed encrypting device according to the circumstances, without an inventive step being involved.

11. The subject matter of Claims 30 and 31 is not inventive in relation to the content of D1 and D3. Claims 30 and 31 therefore do not meet the requirements of PCT Article 33(3).

Claims 30 and 31 relate to a device for decoding a data stream. These claims do not have any additional features in relation to the claims to the encrypting device which could distinguish their subject matter from the cited prior art in an inventive manner.

12. The subject matter of Claims 32 to 34 is not inventive in relation to the content of the cited prior art. Claims 32 to 34 therefore do not meet the requirements of PCT Article 33(3).

Claims 32 to 34 define a method with method steps which correspond to the features of device Claims 25 to 31. The objections raised against Claims 25 to 31 therefore also apply to Claims 32 to 34.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Claims 15 and 16 are dependent on subsequent claims.